Multiparty quantum secret sharing with pure entangled states and decoy photons*

Ping Zhou[1,2,3], Xi-Han Li[1,2,3], Yu-Jie Liang[1,2,3], Fu-Guo Deng[1,2,3†], Hong-Yu Zhou[1,2,3]
[1] *Key Laboratory of Beam Technology and Material Modification of Ministry of Education, Beijing Normal University, Beijing 100875, P. R. China*
[2] *Institute of Low Energy Nuclear Physics, and Department of Material Science and Engineering, Beijing Normal University, Beijing 100875, P. R. China*
[3] *Beijing Radiation Center, Beijing 100875, P. R. China*

(Dated: February 1, 2008)

We present a scheme for multiparty quantum secret sharing of a private key with pure entangled states and decoy photons. The boss, say Alice uses the decoy photons, which are randomly in one of the four nonorthogonal single-photon states, to prevent a potentially dishonest agent from eavesdropping freely. This scheme requires the parties of communication to have neither an ideal single-photon quantum source nor a maximally entangled one, which makes this scheme more convenient than others in a practical application. Moreover, it has the advantage of having high intrinsic efficiency for qubits and exchanging less classical information in principle.

Keywords: Quantum secret sharing; Quantum communication; Pure entangled states; Decoy photons.

PACS numbers: 03.67.Hk, 03.65.Ud

The principles in quantum mechanics, such as the uncertain relation, the correlation of entangled quantum systems and the collapse in quantum measurement, provide some novel ways for secure communication. For instance, quantum key distribution (QKD), whose goal is used to create a private key between two authorized users, has become one of the most mature applications of quantum information techniques [1, 2, 3, 4, 5, 6, 7, 8]. The noncloning theorem forbids a vicious eavesdropper, say Eve, to eavesdrop the quantum information transmitted through a quantum channel freely. The action of Eve will inevitably disturb the quantum systems transmitted and leave a trace in the outcomes obtained by the receiver. The two authorized parties can find out Eve's eavesdropping by comparing a subset of the outcomes in public. This principle has been also applied to other branches of quantum communication, such as quantum secure direct communication[9, 10, 11], deterministic quantum communication [12, 13, 14, 15], quantum secret report [16], quantum broadcast communication[17], quantum secret conference [18], quantum dialogue [19], and so on.

Quantum secret sharing (QSS) is the quantum counterpart of the classical secret sharing. In a secret sharing, a boss, say Alice, has two agents (Bob and Charlie) who are at a remote place, and she wants to send her instruction to her agents for dealing with her business. However Alice suspects that one of her agents may be dishonest, and she does not know who is the dishonest one. Alice believes that the honest one can keep the potentially dishonest from doing harm to her benefits if they both coexist in the process of the business. For the security of the secret message, say M_A, Alice will divide it into two pieces, M_B and M_C, and then sends them to Bob and Charlie, respectively. If and only if Bob and Charlie cooperate, they can read out the message $M_A = M_B \oplus M_C$; otherwise none can obtain a useful information about the secret message. As classical signal is in the eigenvectors of a quantum operator, it can be copied freely and fully. That is to say, it is impossible in principle to share a secret message with classical physics. When quantum mechanics enters the field of information, the story is changed. In 1999, Hillery, Bužek and Berthiaume (HBB99) [20] proposed an original QSS scheme for creating a private key among three parties with a three-particle Greenberger-Horne-Zeilinger (GHZ) state $|GHZ\rangle = \frac{1}{\sqrt{2}}(|000\rangle + |111\rangle)$, the maximally entangled three-particle state. Here $|0\rangle$ and $|1\rangle$ are the two eigenvectors of the measuring basis (MB) Z (for example the z-direction of 1/2-spin). Now, there are a great number of QSS schemes, such as the schemes [20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, 31, 32, 33] for creating a private key and those [34, 35, 36, 37] for sharing an unknown quantum state.

Almost all the existing QSS schemes are based on either maximally entangled quantum signals [20, 21, 22, 23, 24, 25, 26, 27, 28] or an ideal single-photon quantum signal [29, 30, 31, 32, 33], which makes them difficult in a practical application. On one hand, a practical ideal single-photon source cannot be obtained with present techniques although people can in principle produce a single photon. On the other hand, an entangled source usually generates a pure entangled state because of the property of asymmetry in the source.

In this paper, we will present a scheme for quantum secret sharing with pure entangled states, not maximally entangled ones. The boss Alice exploits some decoy photons to forbid a potentially dishonest agent to steal the information

[*] Published in *Physica* A 381 (2007) 164-169.
[†] Email address: fgdeng@bnu.edu.cn

about the private key obtained by another agent. This scheme has the advantage of having high intrinsic efficiency for qubits and exchanging little classical information. Moreover, it does not require the parties of communication to have an ideal single-photon quantum source, which is not available in a practical application with the present techniques, or a maximally entangled quantum source. Thus this QSS scheme is more convenient than others.

Now, let us describe the principle of our QSS scheme. For simplicity, we first describe it with two agents, i.e., Bob and Charlie, and then generalize it to the case with N agents. For the case with two agents, Alice should first prepare a sequence of pure entangled photon pairs S. Each pair is in one of the four states $\{|\phi\rangle_{BC}, |\phi'\rangle_{BC}, |\psi\rangle_{BC}, |\psi'\rangle_{BC}\}$.

$$\begin{aligned} |\phi\rangle_{BC} &= (\alpha|00\rangle + \beta|11\rangle)_{BC}, \qquad (1)\\ |\phi'\rangle_{BC} &= (\alpha|11\rangle + \beta|00\rangle)_{BC}, \qquad (2)\\ |\psi\rangle_{BC} &= (\alpha|01\rangle + \beta|10\rangle)_{BC}, \qquad (3)\\ |\psi'\rangle_{BC} &= (\alpha|10\rangle + \beta|01\rangle)_{BC}, \qquad (4)\end{aligned}$$

where

$$|\alpha|^2 + |\beta|^2 = 1. \qquad (5)$$

Suppose that Alice's entangled source produces an entangled pair in the state $|\phi\rangle_{BC} = (\alpha|00\rangle + \beta|11\rangle)_{BC}$ in each signal interval, Alice can obtain the entangled pair sequence S by operating some of the pairs with the two unitary operations $U_0 = |0\rangle\langle 0| + |1\rangle\langle 1|$ and $U_1 = |1\rangle\langle 0| + |0\rangle\langle 1|$, i.e.,

$$\begin{aligned} |\phi'\rangle_{BC} &= (U_1^B \otimes U_1^C)|\phi\rangle_{BC}, \qquad (6)\\ |\psi\rangle_{BC} &= (U_0^B \otimes U_1^C)|\phi\rangle_{BC}, \qquad (7)\\ |\psi'\rangle_{BC} &= (U_1^B \otimes U_0^C)|\phi\rangle_{BC}. \qquad (8)\end{aligned}$$

Alice divides the sequence S into two sequences S_B and S_C. The sequence S_B is made up of all the B photons of the photon pairs in the sequence S. All the C photons compose of the partner particle sequence S_C, similar to Refs. [7, 9, 10, 11, 12, 13]. Different from the Karlsson-Koashi-Imoto (KKI) QSS scheme [21], the quantum information carries in this scheme are a sequence of pure entangled stats. The photon B and the photon C in a pure entangled state are completely correlated when they are measured with the MB Z, but not with the MB $X = \{|\pm x\rangle = \frac{1}{\sqrt{2}}(|0\rangle \pm |1\rangle)\}$. For instance,

$$\begin{aligned} |\phi\rangle_{BC} &= (\alpha|00\rangle + \beta|11\rangle)_{BC} = \frac{1}{2}[(\alpha+\beta)(|+x\rangle|+x\rangle + |-x\rangle|-x\rangle)\\ &\quad +(\alpha-\beta)(|+x\rangle|-x\rangle + |-x\rangle|+x\rangle)]. \qquad (9)\end{aligned}$$

That is, on one hand, the security of the quantum secret sharing with pure entangled states is lower than that with Bell states if the parties use the two MBs Z and X to measure their photon pairs for the eavesdropping check directly [12]. On the other hand, the quantum source is more convenient than maximally entangled states [12] as the asymmetry in a practical quantum source makes the photon pairs in a pure entangled state, not a maximally one.

For ensuring the security of the transmission of the photon sequences S_B and S_C, Alice should add some decoy photons in these two sequences before she sends S_B and S_C to Bob and Charlie, respectively. The decoy photon technique was proposed first by Li *et al.* [38, 39] in QKD network, and now it has been applied to other branches of quantum communication, such as deterministic secure quantum communication [12], quantum secret report [16] and quantum secret conference [18]. The principle of the decoy photon technique is that Alice prepares some photons which are randomly in one of the four nonorthogonal states $\{|0\rangle, |1\rangle, |+x\rangle, |-x\rangle\}$ and then inserts them into the sequences S_B and S_C. As the states and the positions of the decoy photons are unknown for all the parties of the communication except for Alice herself, the eavesdropping done by an eavesdropper will inevitably disturb these decoy photons and will be detected, similar to Bennett-Brassard 1984 (BB84) protocol [2] and its modified version [8]. The number of the decoy photons is not required to be very large, just large enough for checking eavesdropping. Still, it is unnecessary for Alice to prepare her decoy photons with an ideal single-photon source. She can get them by measuring the photon B in a pure entangled state $|\phi\rangle_{BC}$ and manipulating the other photon C with some unitary operations. For example, if Alice wants to make her decoy photon in the state $|+x\rangle$, she measures the photon B in the pure entangled state $|\phi\rangle_{BC}$ with the MB Z and then performs a Hadamard (H) operation on the photon C when she obtains the outcome $|0\rangle_B$, otherwise she performs the operation $H \otimes U_1$ on the photon C. Here $H = (1/\sqrt{2})(|0\rangle\langle 0| + |1\rangle\langle 0| + |0\rangle\langle 1| - |1\rangle\langle 1|)$. As the analysis of the decoy photons is as same as that in the BB84 QKD protocol [2], our QSS scheme is secure if Alice exploits her decoy photons to forbid the potentially dishonest agent to eavesdrop freely.

Suppose that Alice codes the states $\{|\phi\rangle_{BC}, |\phi'\rangle\}_{BC}$ as 0 and codes the states $\{|\psi\rangle_{BC}, |\psi'\rangle_{BC}\}$ as 1. Our three-party QSS scheme with pure entangled states can work with following steps.

(S1) Alice prepares a sequence of pure entangled two-photon states S, N ordered photon pairs. Each photon pair BC is randomly in one of the four states $\{|\phi\rangle_{BC}, |\phi'\rangle_{BC}, |\psi\rangle_{BC}, |\psi'\rangle_{BC}\}$. She divides the sequence S into two partner particle sequences S_B and S_C. The sequence S_B (S_C) is made up of the photons B (C) in the ordered N photon pairs. Alice prepares $2k$ ($k << N$) decoy photons by measuring the photons B in some photon pairs BC and operating the remaining photons C with the two unitary operations U_i ($i = 0, 1$) and the H operation. She inserts randomly k decoy photons into the sequence S_B and the other k decoy photons into the sequence S_C.

(S2) Alice sends the sequence S_B and S_C to Bob and Charlie, respectively.

(S3) Bob and Charlie measure their photons in the sequences S_B and S_C independently with the two MBs Z and X.

If Bob and Charlie have the capability of storing their quantum states, they can measure their photons in the sequences S_B and S_C in the same way as those in Refs. [9, 10]. That is, Alice first tells Bob and Charlie which are the decoy photons and their states, and then Bob and Charlie measure the decoy photons with the same MBs as those used by Alice for preparing them. For the other photons, Bob and Charlie both choose the MB Z to measure them. In this way, all the decoy photons can be used for checking eavesdropping. The k decoy photons in the sequence S_B (S_C) can be used to check the security of Alice-Bob (Alice-Charlie) quantum line in the same way as the BB84 QKD protocol [2] which has been proven to be secure for generating a private key [40].

Without quantum memory, Bob (Charlie) can measure the photons in the sequence S_B (S_C) in the same way as that used in the modified BB84 QKD protocol [8]. That is to say, Bob (Charlie) measures his photons by using the MB X with the probability p ($p << 1/2$ if N is large enough) and the MB Z with the probability $1 - p$. In this way, half the decoy photons measured by Bob (Charlie) in the sequence S_B (S_C) are useful for checking eavesdropping as the MBs for preparing and measuring them are the same ones. In this time, Alice and Bob (Alice and Charlie) can analyze the error rate of the decoy photons in the sequence S_B (S_C) with the refined analysis technique discussed in the modified BB84 QKD protocol [8]. In detail, they divide the useful decoy photons into two groups, the one they both choose the MB Z and the other one they both choose the MB X. They analyze the error rates of these two groups independently. When the error rates of the two groups of decoy photons both are lower than the threshold η_t, Alice believes that the transmission between her and her agents is secure or the information leaked to a potentially dishonest agent is negligible.

(S4) If Alice confirms that the two quantum lines, i.e., Alice-Bob and Alice-Charlie, both are secure, Alice and her agents distill a private key $K_A = K_B \oplus K_C$ with the other outcomes they all choose the MB Z, similar to QKD [1]; otherwise they repeat their QSS from the beginning. Here K_A, K_B and K_C are the key obtained by Alice, Bob and Charlie, respectively.

As pointed out in Ref. [21], a QSS scheme is secure if it can prevent the potentially dishonest agent from eavesdropping freely. In this QSS scheme, Alice exploits her decoy photons to forbid her agents to eavesdrop freely. As the states and the positions of the decoy photons are unknown for Bob and Charlie, either Bob or Charlie will be detected if he wants to steal the information about the key obtained by the other agent. Thus this QSS scheme can be made to be secure. On the other hand, as the agents choose the MB Z with a lager probability $1 - p$ to measure their photons used for creating the private key, the intrinsic efficiency of qubits $\eta_q \equiv \frac{q_u}{q_t}$ is far larger than that in KKI QSS scheme [21] as p is much smaller than 1/2. Here q_u is the number of the useful qubits and q_t is that of the total qubits transmitted.

It is straightforward to generalize this scheme to the case with M agents, say Bob$_i$ ($i = 1, 2, \cdots, M$). Similar to the case with two agents, Alice prepares a sequence of pure entangled M-photon quantum systems S' (ordered N pure entangled quantum systems), and each quantum system is randomly in one of the four states $\{|\Phi\rangle, |\Phi'\rangle, |\Psi\rangle, |\Psi'\rangle\}$. Here

$$|\Phi\rangle_{B_1B_2\cdots B_M} = (\alpha|00\cdots0\rangle + \beta|11\cdots1\rangle)_{B_1B_2\cdots B_M}, \tag{10}$$

$$|\Phi'\rangle_{B_1B_2\cdots B_M} = (\alpha|11\cdots1\rangle + \beta|00\cdots0\rangle)_{B_1B_2\cdots B_M}, \tag{11}$$

$$|\Psi\rangle_{B_1B_2\cdots B_M} = (\alpha|00\cdots1\rangle + \beta|11\cdots0\rangle)_{B_1B_2\cdots B_M}, \tag{12}$$

$$|\Psi'\rangle_{B_1B_2\cdots B_M} = (\alpha|11\cdots0\rangle + \beta|00\cdots1\rangle)_{B_1B_2\cdots B_M}. \tag{13}$$

Alice divides the sequence S' into M partner photon sequences S'_{B_1}, S'_{B_2}, $\cdots$, and S'_{B_M}. The sequence of S'_i ($i = 1, 2, \cdots, M$) is made up of the photons B_i in all the ordered quantum systems. Also Alice insets randomly k decoy photons, which are prepared by measuring a photon in a pure entangled state and operating the remaining photons with unitary operations U_0, U_1 and H, into each partner photon sequence S_i before she sends it to the agent Bob$_i$. If all the agents have the capability of storing their quantum states, Alice first tells the agents which are the decoy photons and their states in the partner photon sequences when all the agents have received their sequences, and then the agents measure the decoy photons with the same MBs as those used by Alice for preparing them and measure all the pure entangled states with the MB Z. Without quantum memory, the agents should measure their photons in the same way as the case with two agents. That is, all the agents measure their photons by using the MB X with a small probability p and the MB Z with the probability $1-p$. In this time, the rate of the useful qubits to all those transmitted is $p_u = (1-p)^M$. As the same as the case with two agents, the security of each of the partner photons S_i is ensured by the decoy photons, the same as the BB84 QKD protocol [2] or its modified version [8]. In other words, this QSS scheme with N agents can be made to be secure.

As proven by Deng *et al.* [41] that the one-way QSS schemes based on entanglement and a collective eavesdropping check, such as the two famous QSS schemes, the HBB99 QSS scheme and the KKI QSS scheme, are insecure with a lossy quantum channel if the parties only exploit the correlation of the entangled quantum systems to check eavesdropping, this QSS scheme is an optimal one. It has the following advantages obviously: (a) The quantum signals are a sequence of pure entangled states, not maximally entangled ones, which makes it more convenient than others in a practical application. (b) The boss Alice exploits some decoy photons to ensure the security of this scheme, which is just the requirement of a secure one-way QSS scheme based on entanglement and a collective eavesdropping check in a practical application [41]. (c) It requires the boss has neither an ideal single-photon quantum signal source nor a maximally entangled source. (d) It does not requires the parties exchange a large number of classical information as the agents choose a large probability to measure their photons with the MB Z. (e) Its intrinsic efficiency for qubits is very high, approaching 100% when the number of bits in the private key K_A is large enough.

In conclusion, we have presented a QSS scheme with pure entangled states and decoy photons. As this scheme requires the parties to have neither an ideal single-photon quantum source nor a maximally entangle one, it is more convenient in a practical application than others. Whether the agents have quantum memory or not, this scheme has the advantage of having a high intrinsic efficiency for qubits and exchanging little classical information. For a one-way QSS based on entanglement and a collective eavesdropping check, it is useful for the boss Alice to make at least the qubits used for checking eavesdropping in single-particle states, not entangled ones [41]. Thus this scheme with decoy photons is an optimal one.

This work is supported by the National Natural Science Foundation of China under Grant Nos. 10604008 and 10435020, and Beijing Education Committee under Grant No. XK100270454.

[1] N. Gisin, G. Ribordy, W . Tittel, H. Zbinden, Rev. Mod. Phys.74 (2002) 145.

[2] C. H. Bennett, G. Brassard, in: Proceeding of the IEEE International Conference on Computers, Systems and Signal Processing, Bangalore, India, IEEE, New York, 1984, P. 175.

[3] A. K. Ekert, Phys. Rev. Lett. 67 (1991) 661.

[4] C. H. Bennett, G. Brassard, N. D. Mermin, Phys. Rev. Lett. 68 (1992) 557.

[5] F. G. Deng, G. L. Long, Phys. Rev. A 68 (2003) 042315.

[6] F. G. Deng, G. L. Long, Phys. Rev. A 70 (2004) 012311.

[7] G. L. Long, X. S. Liu, Phys. Rev. A 65 (2002) 032302.

[8] H. K. Lo, H. F. Chau, M. Ardehali J. Cryptology 18 (2005) 122.

[9] F. G. Deng, G. L. Long, X. S. Liu, Phys. Rev. A 68 (2003) 042317.

[10] F. G. Deng, G. L. Long, Phys. Rev. A 69 (2004) 052319.

[11] C. Wang, F. G. Deng, Y. S. Li, X. S. Liu, G. L. Long, Phys. Rev. A 71 (2005) 044305; C. Wang, F. G. Deng, G. L. Long, Opt. Commun. 253 (2005) 15.

[12] X. H. Li, F. G. Deng, C. Y. Li, Y. J. Liang, P. Zhou, H. Y. Zhou, J. Korean Phys. Soc. 49 (2006) 1354.

[13] X. H. Li, F. G. Deng, H. Y. Zhou, Phys. Rev. A 74 (2006) 054302.

[14] Z. X. Man, Z. J. Zhang, Y. Li, Chin. Phys. Lett. 22 (2005) 18; F. L. Yan, X. Zhang, Euro. Phys. J. B 41 (2004) 75; T. Gao, F. L. Yan, Z. X. Wang, Chin. Phys. 14 (2005) 893.

[15] Q. Y. Cai, B. W. Li Chin. Phys. Lett. 21 (2004) 601; A. D. Zhu, Y. Xia, Q. B. Fan, S. Zhang, Phys. Rev. A 73 (2006) 022338; J. Wang, Q. Zhang, C. J. Tang, Phys. Lett. A 358 (2006) 256; H. J. Cao, H. S. Song, Chin. Phys. Lett. 23 (2006) 290.

[16] F. G. Deng, X. H. Li, C. Y. Li, P. Zhou, Y. J. Liang, H. Y. Zhou, Chin. Phys. Lett. 23 (2006) 1676.

[17] J. Wang, Q. Zhang, C. J. Tang, quant-ph/060179.

[18] X. H. Li, C. Y. Li, F. G. Deng, P. Zhou, Y. J. Liang, H. Y. Zhou, Chin. Phys. Lett. 24 (2007) 23.

[19] B. A. Nguyen, Phys. Lett. A 328 (2004) 6.

[20] M. Hillery, V. Bužek, A. Berthiaume, Phys. Rev. A 59 (1999) 1829.

[21] A. Karlsson, M. Koashi, N. Imoto, Phys. Rev. A 59 (1999) 162.

[22] L. Xiao, G. L. Long, F. G. Deng, J. W. Pan, Phys. Rev. A 69 (2004) 052307; F. G. Deng, P. Zhou, X. H. Li, C. Y. Li, H. Y. Zhou, Chin. Phys. Lett. 23 (2006) 1084.

[23] V. Karimipour, A. Bahraminasab, S. Bagherinezhad, Phys. Rev. A 65 (2002) 042320.

[24] C. P. Yang, J. Gea-Banacloche, J. Opt. B: Qantum Semiclass. Opt. 3 (2001) 407.

[25] S. Bandyopadhyay, Phys. Rev. A 62 (2000) 012308.

[26] F. G. Deng, G. L. Long, H. Y. Zhou, Phys. Lett. A 340 (2005) 43; F. G. Deng, X. H. Li, C. Y. Li, P. Zhou, H. Y. Zhou, Phys. Lett. A 354 (2005) 190.

[27] P Chen, F. G. Deng, G. L. Long, Chin. Phys. 15 (2006) 2228.

[28] Z. J. Zhang, Physica A 361 (2006) 233.

[29] G. P. Guo, G. C. Guo, Phys. Lett. A 310 (2003) 247.

[30] F. G. Deng, H. Y. Zhou, G. L. Long, Phys. Lett. A 337 (2005) 329; F. G. Deng, H. Y. Zhou, G. L. Long, J. Phys. A 39 (2006) 14089.

[31] F. L. Yan, T. Gao Phys. Rev. A 72 (2005) 012304.

[32] Z. J. Zhang, Y. Li, Z. X. Man, Phys. Rev. A 71 (2005) 044301.

[33] F. G. Deng, X. H. Li, H. Y. Zhou, Z. J. Zhang, Phys. Rev. A 72 (2005) 044302.

[34] Y. M. Li, K. S. Zhang, K. C. Peng, Phys. Lett. A 324 (2004) 420.

[35] F. G. Deng, C. Y. Li, Y. S. Li, H. Y. Zhou, Y. Wang, Phys. Rev. A 72 (2005) 044301; F. G. Deng, X. H. Li, C. Y. Li, P. Zhou, H. Y. Zhou, Phys. Rev. A 72 (2005) 022338.

[36] X. H. Li, P. Zhou, C. Y. LI, H. Y. Zhou, F. G. Deng, J. Phys. B 39 (2006) 1975; F. G. Deng, X. H. Li, C. Y. Li, P. Zhou, H. Y. Zhou, Eur. Phys. J. D 39 (2006) 459.

[37] Z. J. Zhang, Eur. Phys. J. D 33 (2005) 133; Y. Q. Zhang, X. R. Jin, S. Zhang, Chin. Phys. 15 (2006) 2252.

[38] C. Y. Li, H. Y. Zhou, Y. Wang, F. G. Deng, Chin. Phys. Lett. 22 (2005) 1049.

[39] C. Y. Li, X. H. Li, F. G. Deng, P. Zhou, Y. J. Liang, H. Y. Zhou, Chin. Phys. Lett. 23 (2006) 2896.

[40] H. K. Lo, H. F. Zhau, Science 283 (1999) 2050; P. W. Shor, J. Preskill, Phys. Rev. Lett. 85 (2000) 441.

[41] F. G. Deng, X. H. Li, H. Y. Zhou, arXiv: 0705.0279.